Results 1 - 10 of about 252. (0.08 sec)

New public-key cryptosystem using **braid** groups — psu.edu [PDF]
KH Ko, SJ Lee, JH Cheon, JW Han, J Kang, C ... - Lecture Notes in ..., 2000 - Springer
... design. Key words: public key cryptosystem, **braid group**, **conjugacy** problem, key exchange, hard problem, non-commutative **group**, one-way function, public key infrastructure 1 Introduction 1.1 Background and Previous Results ...
Cited by 184 - Related articles - BL Direct - All 18 versions

[PDF] New **signature** scheme using **conjugacy** problem — psu.edu [PDF]
KH Ko, DH Choi, MS Cho, JW Lee - preprint, 2002 - Citeseer
... We propose a new **digital signature** scheme based on a non-commutative **group** where the **conjugacy** search problem is hard and the **conjugacy** decision problem is feasible. We implement our **signature** scheme in the **braid** groups and prove that an existential forgery of the ...
Cited by 38 - Related articles - View as HTML - All 6 versions

Group signature schemes using **braid** groups — arxiv.org [PDF]
T Thomas, AK Lal - Arxiv preprint cs/0602063, 2006 - arxiv.org
... schemes based on the **conjugacy** problem, decomposition problem and root problem in the **braid** groups which are believed to be hard problems. Key Words: **braid group**, **braid** cryptography, **digital signature**, **group signature** 2000 MSC: Primary: 94A60; Secondary: 20F36 ...
Cited by 10 - Related articles - View as HTML - All 3 versions

... protocol (KAP) using **conjugacy** and discrete logarithm problems in **group** ... — mii.lt [PDF]
E Sakalauskas, P Tvarijonas, A Raulynaitis - Informatica, 2007 - IOS Press
... Preprint, Basel. Available at: www.math.unibas.ch Long, D. (1994). Constructing representations of **braid** groups. Comm. Anal. ... Combinatorial **group** theory and public key cryptography. ... The **conjugacy** search problem in public key cryptography: unnecessary and insufficient. ...
Cited by 7 - Related articles - All 5 versions

[PDF] Blind **signature** scheme over **braid** groups — iacr.org [PDF]
GK Verma - Preprint, http://eprint. iacr. org/2008/027, 2008 - eprint.iacr.org
... Blind **signatures** are the basic tools of **digital** cash payment systems, electronic voting systems ...

we give a brief description of **braid** groups and computationally hard problems regarding **conjugacy**. ... 2. **Braid Group** and **Conjugacy** Problem: In this section we give a brief description ...
Cited by 5 - Related articles - View as HTML - All 2 versions

One **digital signature** scheme in semimodule over semiring [mii.lt [PDF]]
E Sakalauskas - Informatica, 2005 - IOS Press
... Ki Hyoung, Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, Choonsik Park (2000). New public-key cryptosystem using **braid** groups. ... New **Signature** Scheme Using **Conjugacy** Problem. ... Magnus, W., A. Karrass, D. Solitar (1966). Combinatorial **Group** Theory. ...
Cited by 8 - Related articles - All 5 versions

New public key cryptosystem using finite non abelian groups [psu.edu [PDF]]
SH Paeng, KC Ha, JH Kim, S Chee, C Park - Lecture notes in computer ..., 2001 - Springer
... 471 – We can apply our encryption scheme to G even if DLP and the (special) **conjugacy** problem in G ... It is easy to make a **signature** scheme with our PKC: In general, it is not easy to find a **signature** scheme using an infinite non abelian **group** such as a **braid group** [11]. ...
Cited by 32 - Related articles - BL Direct - All 7 versions

[PDF] Provably-Secure Identification Scheme based on **Braid Group** [kaist.ac.kr [PDF]]
Z Kim, K Kim - Proceedings of the international conference on ..., 2004 - caislab.kaist.ac.kr
... construction of a new identification scheme based on the **conjugacy** problem on the **braid group**. ... J. Han, J. Kang, C. Park, "New Pulic-key Cryptosystem using **Braid** Groups," Advances ... DH Choi, MS Cho, and JW Lee, " New **signature** scheme using **conjugacy** problem," Preprint ...
Cited by 7 - Related articles - View as HTML - All 3 versions

[PDF] A proxy **signature** scheme over **braid** groups [iacr.org [PDF]]
GK Verma - 2008-05-18]. http://eprint. iaer. org/2008/160. pdf - eprint.iacr.org
... In 2002 a **signature** scheme [10] was given by Ko et al using **conjugacy** problem. In 2008 [12], a blind **signature** scheme over **braid group** has been proposed by GK Verma. Several other **digital signature** schemes have also been proposed but no proxy **signature** scheme has ...
Cited by 3 - Related articles - View as HTML - All 2 versions

[PDF] Post-quantum **signatures** [psu.edu [PDF]]
J Buchmann, C Coronado, M Döring, D Engelbert, C ... - Preprint, 2004 - Citeseer
... (a) by demanding that the conjugating element come from a certain sub- **group** of B n . The resulting ... The resulting problem is called the Multiple **Conjugacy** Search Problem (MCSP). 11 Page 13. Alternatively, one may use the weaker **Braid** Diffie-Hellman Problem (BDHP). ...
Cited by 5 - Related articles - View as HTML - All 11 versions

Gooooooooogle ▶

Result Page: 1 2 3 4 5 6 7 8 9 10 Next

braid group conjugacy digital signati Search

Go to Google Home - About Google - About Google Scholar